

Hizballah: Deception in the 2006 Summer War

By David A. Acosta, Major, USA

Editorial Abstract: Major Acosta describes the contemporary Hizballah-Israeli conflict, then provides a extensive analysis of successful deception practices used in the recent campaign. He evaluates use of several information operations core competencies, and explains how traditional deception methods remain relevant in the modern battlespace.

The 2006 summer conflict between Israel and Hizballah was six years in the making. As it played out, certain things became quite clear: Hizballah was ready, Israel was not. Over and over again as the war unfolded not only in southern Lebanon but on the televisions and computers of the rest of the world, the power of Hizballah's deception plan played out. Key to their success was use of deception in support of their overall strategy. Using all means available, Hizballah prosecuted the conflict with very successful results. As one reporter describes:

From the onset of the conflict to its last operations, Hizballah commanders successfully penetrated Israel's strategic and tactical decision-making cycle across a spectrum of intelligence, military and political operations, with the result that Hizballah scored a decisive and complete victory in its war with Israel.

Prior to launching a discussion on the actual deception campaign, this article examines those events leading up to the conflict, as well as describing the other critical piece—Hizballah's use of denial in the conflict. Demonstrating effectiveness of this element makes it easier to show how well their deception worked. Criteria used to evaluate Hizballah's acts include the objectives and categories of deception listed by Daniel & Herbig, the techniques listed by Dunnigan and Nofi, and the sensors utilized to pass the information or signal. Table 1 shows example deception evaluation criteria.

Background

Since its creation in the early 1980s, Hizballah has been fighting a guerrilla-type war against Israel. In 1985,

following a nearly three year occupation of most of Lebanon south of Beirut, Israel pulled out of much of Lebanon into a security zone along its northern border. While Israel hoped to stabilize its northern border, Hizballah remained persistent with attacks against Israeli military targets in this area. Twice Israel launched sustained ground offensives outside of their self-proclaimed security zone, in attempts to stop Hizballah's attacks.

The IDF launched Operation Accountability in 1993 with the intent of putting pressure on Syrian and Lebanese forces to weaken Hizballah, but to no avail. The second operation, launched in 1996 as Operation Grapes of Wrath, was again aimed at putting pressure on Syrian and Lebanese forces to weaken Hizballah, and it too failed. By the end of the 1990s following nearly two decades of conflict, Israel unilaterally withdrew from its southern security zone in Lebanon after the loss of nearly 1,500 soldiers and low public support for the mission. This withdrawal, as Avi Jorish points out in his book *Beacon of Hatred*, "led many to believe that Hizballah had defeated Israel, and the party's reputation consequently soared throughout the entire Arab world." Following the pullback, Israel and Hizballah engaged in a 'quasi peace' along the southern Lebanese border known commonly as the "Blue Line," monitored by members of the United Nations Interim Force in Lebanon (UNIFIL).

A phony war developed on the Blue Line between Israel and Lebanon. Nicholas Blanford in *Jane's Intelligence Review* describes the situation between Hizballah and the IDF in a report from 2006: "The IR [Islamic Resistance]

Criteria
Three Objectives ? - Condition the target's beliefs ? - Influence the target's actions ? - Target's actions must benefit the deceiver ?
Sensors targeted ?
Type: M-type (Misleading) or A-type (Ambiguity) ?
9 Characteristics ? (concealment, camouflage, false and planted information, ruses, displays, demonstrations, feints, lies, and insight)

Table 1. Deception Evaluation Criteria

had been attacking the IDF along the Blue Line for six years in a finely calibrated campaign of periodic hit-and-run raids, roadside bombings and artillery bombardments." The goal of these actions was, as Blanford describes, to "maintain pressure on the IDF without provoking Israel into a massive retaliation that could harm Hizballah's domestic popularity." Furthermore, in an effort to gain the release of its own Israeli held prisoners, Hizballah began a new strategy: the kidnapping of Israeli soldiers. The group made five attempts before the July 2006 kidnappings to abduct IDF personnel. Frustrated by Hizballah's previous actions, Israel "had enough," and a senior IDF leader stated to the UNIFIL commander that if Hizballah attempted another kidnapping, "we will burn Beirut." While this information was passed on to the Lebanese government, no one is certain if it reached Hizballah's leadership. Thus, the situation was quite tense by the early summer of 2006.

Even in the days leading up to the 12 July incident, Hizballah's leadership,

aware of the importance of the tourist season to Lebanon's economy, reassured Lebanese Prime Minister Fouad Siniora that Hizballah would take no actions against Israel. Meanwhile, standing orders to Hizballah's Islamic Resistance units along the Blue Line went unchanged: "exploit Israeli military weaknesses" and abduct IDF soldiers given the opportunity. Under these circumstances both sides stood poised for a clash on the morning of 12 July 2006.

At a little after nine in the morning local time, an IDF patrol consisting of two "Hummvee" type-vehicles came under fire from IR forces along the Blue line. Within minutes, the patrol—out of communication range with higher headquarters and in a blindspot from IDF covering fire—had two dead, three wounded and Eldad Regev and Ehud Goldwasser lay in Hizballah's hands. In the following hours, both Hizballah and the IDF embarked on a series of skirmishes along the border resulting in several Israeli soldiers killed and injured. In Beirut senior Hizballah leaders attempted to calm Lebanese officials' fears about Israeli reprisals, even going as far as to speak to the Prime Minister and Minister of the Interior. Unlike previous attempts, this time Israel did react swiftly.

Within hours Israeli warplanes attacked Hizballah positions along the Blue Line and destroyed several bridges on the Litani River, in an attempt to isolate the southwest portion of the country. As a response, Hizballah began to unleash scores of Katyusha rockets into northern Israel. A new chapter in the battle between Israel and Hizballah had begun.

As the bullets and rockets began to fly across the border, both sides identified strategic objectives for the conflict. Anthony Cordesmen from the Center for Strategic and International Studies, points out that from the onset of hostilities the Israeli Cabinet under the direction of Prime Minister Ehud Olmert laid out five key Israeli objectives for the war:

- Destroy the "Iranian Western Command" before Iran could go nuclear.

- Restore the credibility of Israeli deterrence after the unilateral withdrawal from Lebanon in 2000 and Gaza in 2005, and countering the image that Israel was weak and forced to leave.

- Force Lebanon to become and act as an accountable state, and end the status of Hizballah as a state within a state.

- Damage or cripple Hizballah, with the understanding that it could not be destroyed as a military force and would continue to be a major political actor in Lebanon.

- Bring the two capture Israeli soldiers back alive without major trades in prisoners held by Israel.



*Beirut during the 2006 Summer War.
(Defense Link)*

On the other side, Hizballah had its own objectives. Their main goal lay in humiliating Israel by sheer survival, as Hizballah's Secretary-General Hassan Nasrallah pointed out in an interview on 21 July. Nasrallah claimed "the victory we are talking about is when the resistance survives. When its will is not broken, then this is a victory." While not much else is known of their objectives, because of the tight security within Hizballah, perhaps another can be found in Ron Schliefer's piece, "Psychological Operations: A New Variation of an Age Old Art: Hizballah versus Israel." Schliefer describes psychological warfare executed by

Hizballah in their campaign to push Israel out of southern Lebanon, leading up to the 2000 withdrawal. Schliefer exerts "[Hizballah] launched a... guerilla war psychologically waged," meaning the organization attacked IDF soldiers not to conquer land, but as an end in itself. By drawing out and killing Israeli soldiers, Hizballah's objective was reducing Israeli morale and public opinion to the point where the IDF would withdraw—as they had done in 2000. Thus, much of the Hizballah's battle plan lay in the use of information operations to wear down Israel.

The war played out on land, in the air, and at sea across Lebanon and northern Israel. Shortly after the commencement of hostilities, Israel began a naval blockade of Lebanese ports, hoping to cut off arms shipments to Hizballah. The Israeli Air Force (IAF) launched what seemed like a brutal series of attacks, first aimed at Hizballah missile and rockets sites in southern Lebanon, but then turning on critical Lebanese infrastructure. This included crucial road intersections, bridges, and even the Beirut airport, in images reminiscent of Lebanon in the mid-1980s. Despite the IAF's destruction of 54 long range rocket and missile launch sites in 39 minutes, on the first day of the conflict, Hizballah continued a daily rain of shorter range Katyusha rockets on Israel's northern towns and villages. By the end of the first 72 hours, Israel's air campaign showed little results of degrading Hizballah's capabilities, and the chances of Israel achieving a decisive victory became increasingly—and highly—unlikely.

By 17 July, Israel turned to the ground option to combat Hizballah in the south of Lebanon. Land forces yielded little more than the air option, as IDF forces quickly found that the guerrilla force in front of them was quite exceptional. "We didn't know what hit us," observed one IDF soldier in a *Sunday Times* interview, "In seconds we had two dead." As units pushed north, many found themselves surrounded at times, fighting a true asymmetric threat as guerrillas swarmed seemingly from all sides with anti-tank missiles and other weapons. Because of this slow going,

the ground war had to be expanded to account for the problems Israeli forces faced as their “blitzkrieg” style assault ground to a halt.

In early August, with Israel unable to score a decisive victory, the UN pushed all sides in the conflict towards a cease-fire. On 14 August, both Hizballah and Israel agreed to the cease-fire proposal and the guidelines of UN resolution 1701. In 34 days of fighting Israel sent nearly 30,000 soldiers to fight in southern Lebanon, while reports of Hizballah’s numbers are considerably less, perhaps as low as 3000, or just one brigade’s worth of militia. Even on the last day before the cease-fire, Hizballah rockets and missiles continued to rain down on Israel, despite all prior Israeli actions. UN Resolution 1701 provided that the Lebanese Army, under the observation of increased UNIFIL force would ensure Hizballah leaves southern Lebanon, the likes of which remain to be seen. At the termination of hostilities little had changed, and Hizballah was left still standing, deception having played a key role at the tactical and operational levels to shape the outcome of the battle.

Hizballah’s Denial Operations

Even before the conflict started, Hizballah began its campaign to control the information battlespace with Israel. The group’s ability to maintain operational security, and deny Israel the critical information it would need to adjust its battleplans during the course of the conflict, would have significant repercussions. By controlling the information environment, Hizballah in effect dictated the rules of the game. Key to denial is having access to the enemy’s sensors. There are two strikingly different examples of how Hizballah targeted Israeli sensors and exploited them to support the war effort. The first comes through more traditional means, namely the use of spies. The second, broader example, deals with the accessibility of information in a closed society versus an open one. Both methods of denial significantly contributed to both the war effort, and the deception plans employed throughout.

The use of spies is one of the oldest methods of intelligence gathering known in warfare and Hizballah made good use of it. Significantly, Hizballah’s agents made major inroads in the previous ten years of counterintelligence efforts against Israel, and in the summer of 2006 this work paid off. In an *Asia Times* article, authors Alistair Crooke and Mark Perry write “over a period of two years, Hizballah’s intelligence officials had built a significant signals-counterintelligence capability... Hizballah had identified key Israeli human-intelligence assets in Lebanon.” They add that in the month before the abduction of the two IDF personnel, the Lebanese government—with assistance from Hizballah—broke up an Israeli spy ring inside Lebanon. Finally, Crooke and Perry remark that “Hizballah had successfully ‘turned’ a number of Lebanese civilian assets reporting on the location of major Hizballah military caches in southern Lebanon to Israeli intelligence officers.”

These actions, which had dire consequences for the Israelis, were critical to Hizballah’s deception plan. In effect they effectively closed down Israel’s human intelligence capability, often regarded for its “intelligence dominance” in previous conflicts with its Arab neighbors. The other key element to Hizballah’s denial campaign involved the high degree of internal security within this organization. As a “state within a state,” Hizballah demonstrated a high level of security among its members, using two primary ways to control its information footprint. The first involves its soldiers and militia on the ground. So secretive were Hizballah preparations for the conflict, reportedly “no single commander knew the location of each bunker” from which they would be fighting. Additionally, after being hidden during several attempts on his life, Secretary General Hassan Nasrallah remarked on how good Hizballah’s security apparatus was, noting “Not even I knew where I was.”

Alongside the individual security and denial that Hizballah exhibited, they tightly controlled open source

information coming out of Lebanon. This allowed Hizballah to tell their story better than Israel, because there was only one story to tell and then only told by a few high ranking people in Hizballah’s organization. Hizballah’s information campaign opens a debate in some circles on lessons from the war. Marvin Kalb describes it this way: *If we are to collect lessons from this war, one of them would have to be that a closed society can control the image and the message that it wishes to convey to the rest of the world far more effectively than can an open society, especially one engaged in an existential struggle for survival. An open society becomes victim of its own openness... A closed society conveys the impression of order and discipline; an open society, buffeted by the crosswinds of reality and rumor, criticism and revelation, conveys the impression of disorder, chaos and uncertainty...*

Hizballah never admitted how many casualties it took during the fighting, another indicator of the high level of security it maintains. Thus having a closed society with tight control over the media picture greatly enhanced Hizballah’s ability to control information broadcast to the rest of the world.

This closed society greatly contributed to their overall denial capabilities because it produced a limited information signature, greatly restricting Israel’s ability to obtain open source information. Again and again throughout the conflict, these two key denial operations would be very significant, not only within the overall conflict—but more importantly to this discussion—Hizballah’s deception operations. By examining these operations in depth, and evaluating their effectiveness, Hizballah’s successes become even clearer.

Battle Plans

As mentioned earlier, after the first 72 hours of Israeli airstrikes against targets across Lebanon, IDF leaders decided to begin limited ground incursions into southern Lebanon. The Israelis very quickly discovered they were in for a surprise. Hizballah began

preparing its future battle plan on the heels of Israel's earlier withdrawal from southern Lebanon, in 2000.

Hizballah undertook an elaborate construction effort of display fortifications along the Blue Line, with the intent of deceiving information gathering assets such as Israeli unmanned aerial vehicles (UAV), UNIFIL observers and Lebanese spying for Israel. Meanwhile, in secret locations out of sight of information gathering assets, Hizballah built their real bunkers. It was a classic example of military deception; Hizballah purposely lured observers into believing that the openly visible bunkers should be targeted if conflict occurred. *Asia Times* reporters Alistair and Crooke note

that at the same time, Hizballah's construction of real bunkers went forward "in areas kept hidden from the Lebanese population." They go on to add that "Nearly 600 separate ammunition and weapons bunkers were strategically placed in the region south of the Litani." When asked about these bunkers, Senior IDF commanders reported that "It's a very hilly area and its not easy. You cannot identify their bunkers until you're right there." The tunnels and bunkers built in view of Israeli and UNIFIL observers, along with the targets fed back to Israel through Hizballah's counterintelligence operations, identified key emplacements that did not, in fact, exist. As one former UNIFIL observer describes "We were meant to see these things... They were not making any effort to stop us looking... they really fooled us on that one." In comparison to the decoy bunkers another UNIFIL officer reported to *Janes* on the real bunkers: "We never saw them build anything. They must have brought the cement in by the spoonful." The bunker deception was reinforced by the tight secrecy that Hizballah maintained through all the years leading up to the battle. Thus when

Israel again crossed over into southern Lebanon, much of the intelligence driving their planning proved false, and Israeli ground forces paid the price for this intelligence failure.

Evaluating this case of tactical deception shows just how successful it really was. Furthermore, based on the Dunnigan & Nofi's examples, these fake bunkers are prime examples of "displays," in that they attempt to "make the enemy see what isn't there" and that "you're simply attempting to make it appear other than what it really is." Looking at the type of deception (Table 2), using the Daniel & Herbig's model, these fake bunkers fall into the realm of

Criteria	Evaluation
Three Objectives? - Condition the target's beliefs? - Influence the target's actions? - Target's actions must benefit the deceiver?	- Israel felt it knew where Hizballah's bunkers were and attacked them early on. - Hizballah was able to operate from the real bunkers with little threat from Israeli attacks
Sensors targeted?	Israeli UAVs, UNIFIL observers, Lebanese spies.
Type: M-type or A-type?	M-type: the fake bunkers served to mislead the IDF's attacks.
9 Characteristics? (concealment, camouflage, false and planted information, ruses, displays, demonstrations, feints, lies, and insight)	Display: making the enemy see what isn't there. Israel and UNIFIL saw bunkers but did not see the real bunkers until combat began

Table 2. Evaluation of Bunker Deception

misleading or 'M-type' because these displays took attention off of the main effort: Hizballah's construction and defense of the real bunker system. The overall effectiveness can be measured in the statements above taken from UNIFIL representatives and IDF leaders, in that they knew virtually nothing about the extent of the real bunkers, and focused almost entirely on the fake ones. This case serves as a textbook example of tactical deception in warfare.

Electronic Warfare Bluff

Another successful use of deception, Hizballah's electronic warfare (EW) bluff also contributed to their overall battle plan. From the onset it appeared Hizballah was using a new, previously unseen weapon in the conflict between

it and Israel: EW. Reports suggest Hizballah, probably assisted with Iranian supplied technology, was able to intercept Israel's secure frequency hopping radio transmissions, monitoring information on troop movements, casualty reports and supply routes. As one Israeli officer claims, "They monitored our secure communications in the most professional way," adding that Hizballah would "send it [casualties' names] to their Al-Manar TV, which broadcast it almost live, long before the official Israeli radio." This action clearly represented an effective use of PSYOP as well, designed to erode popular support for the war back in Israel. The alleged sophistication of

these electronic attacks underscored how "the Shia group had higher military capabilities" than many in Israel and the United States originally thought.

While Israel did not publicly comment on what it did to counter this threat, Hizballah's EW attacks prompted one former Israeli general to remark that the group's listening capabilities had "disastrous" consequences for Israel's offensive in southern Lebanon. The

news of Hizballah's EW attacks and penetration of Israel's secure airwaves have since proven untrue. During and immediately following the conflict both US and Israeli technicians examined the problem of whether or not Hizballah could actually listen in to supposedly secure frequency-hopping technology. In *Aviation Week & Space Technology* author David Fulghum paints a more realistic picture—and the title says it all: "Doubt as a Weapon." The first to expose this deceptive act, Fulghum noted "Hizballah is incapable of penetrating and exploiting the Israeli army's tactical radio systems as it claimed it did during the recent fighting in Lebanon," pointing to senior US electronics officials for reference. The author continues: *What they're really doing is a very good*

psychological operations... one of the things you want to do is instill doubt. Hizballah makes the pronouncement that they can read encrypted radios. They wanted the IDF troops to believe they weren't as invulnerable as they thought. It ran like wildfire through the US troops as well. What you're witnessing is unsophisticated technology exploited by sophisticated information operations. They scored big time in the psychological warfare department the enemy is figuring out ways to use the information age against us.

The article points out what most likely occurred: confusion by other news agencies, in which reporters “confused cell-phone and frequency hopping radio technology.” Listening into cell phones is a “basic signals intelligence technique”—easily accomplished since “everybody out there has a cell phone.”

In what might be considered part of the EW bluff, UNIFIL supplied another bit of evidence regarding Israel's vulnerabilities. In his piece on the media's role in the 2006 conflict, Marvin Kalb argues UNIFIL “published information on its official website about Israeli troop movements, information that in military circles would be regarded as ‘actionable intelligence.’” He provides examples such as key IDF units being reinforced, types of equipment traveling across the border, and which directions these units headed on various days during the battle. While it is impossible to know for certain whether Hizballah acted on the information provided by UNIFIL, Kalb suggests it would be silly not to consider this as a prime Hizballah intelligence source. Having already seen the resilience of Hizballah in preparing the defense of southern Lebanon, and knowing they have an organic OSINT capability, one cannot put it past this organization to use these sources to help put together a very credible EW deception.

Hizballah's EW bluff serves as another effective use of deception in this conflict, highlighting their capability to conduct more sophisticated information operations as well. While this seems to be more of a problem for Israel at the

tactical level, it has operational level implications as well: specifically, it forced Israel to rethink its communications network in the wake of Hizballah's alleged EW capabilities. Again, this is a case of a misleading deception type, whereby Hizballah sought to convince Israel of “the attractiveness of one wrong alternative”—that their communication system security had been compromised. Hizballah's dissemination system passed false and planted information through sources like Al-Manar, and other media outlets and reports. While Israeli statements clearly show they were convinced Hizballah could listen into their radios, it is unknown how the IDF responded—but it most likely had the psychological effect of painting them as



*Lebanese “call for help” message.
(Associated Press)*

no longer invulnerable. Furthermore, on the objective of being able to benefit from the target's actions, Hizballah made out in a more subtle way. As the fight continued and casualties mounted, many reservists called up for the war began to wonder why they were being sent out as cannon fodder into Hizballah-controlled villages, instead of air strikes going in first. An 11 August 2006 survey conducted by an Israeli newspaper found that 91% of respondents felt the IDF should bomb villages to take out Hizballah, versus only 8% who felt that ground forces should be used instead. The results only served to benefit Hizballah because of their control of the story inside Lebanon.

Israeli ground and air campaigns would only further allow Hizballah to paint a picture of “disproportionately” of Israeli acts. With all of these results in mind, the EW bluff successfully benefited Hizballah's overall campaign plan. Table 3 summarizes this example.

Another key lesson from this example are the linkages between various information activities. Like many deception operations, while Hizballah bluffed about their exact capabilities, a certain amount of truth existed in the lie. They successfully exercised electronic warfare by being able to listen into Israeli cell phones, and exploiting other information sources as part of the deception. Hizballah also used information broadcast on Al-Manar for PSYOP purposes. Finally, Fulghum describes this deception tactic as having PSYOP implications, because Hizballah “wanted the IDF troops to believe they weren't as invulnerable as they thought” The same effect “ran like wildfire through the US troops as well.” Only months after the conflict, when engineers explained the impossibility of the act, did Israeli and US fears subside. But by that time, the damage was done.

Media & The Battle of the Story

One of most remembered aspects of the 2006 Summer Conflict will be the media's role in the war. Hizballah's use of media shows just how effective it can be in modern deception operations. Radio, TV and the Web became a primary weapon against Israel, and a key deception tool. Marvin Kalb describes it this way:

During the summertime war in Lebanon, it [the Internet] helped produce the first really “live” war in history... not until this war have networks actually projected in real time the grim reality of the battlefield—pictures of advancing or retreating Israeli troops in southern Lebanon, homes and villages being destroyed during bombing runs, old people wandering aimlessly through the debris, some tailed by children hugging tattered dolls, Israeli airplanes attacking Beirut airport, Hizballah rockets striking northern Israel and Haifa, forcing

Criteria	Evaluation
Three Objectives? - Condition the target's beliefs? - Influence the target's actions? - Target's actions must benefit the deceiver?	- Israel thought Hizballah could listen to secure radio communication. Hizballah forced Israel to re-look their actions. - Hizballah appeared to be stronger than it really was through this act.
Sensors targeted?	Media, open source intelligence
Type: M-type or A-type?	M-type: this bluff the attractiveness of one wrong alternative (the capability to listen to secure radio comms)
9 Characteristics? (concealment, camouflage, false and planted information, ruses, displays, demonstrations, feints, lies, and insight)	Lies: While able to listen to cell phones, Hizballah could not listen to secure radio communications, but said they could.

Table 3. Evaluation of EW Bluff

300,000 to evacuate their homes and move into underground shelters—all conveyed “live,” as though the world had a front-row seat on the blood and gore of modern warfare.

Kalb adds that because so much information was now available to the media and the public, a shift in information flow occurred. “Once upon a time,” he writes, “such information was the stuff of military intelligence acquired with considerable efforts and risk; now it has become the stuff of everyday journalism. The camera and the computer have become weapons of war.”

Hizballah realized the power of manipulated media years before the conflict, and exploited this to the fullest during this war. Hizballah’s use of the media shows where deception can be found in information warfare. Essentially, Hizballah’s deception operations utilized the media to conceal the locations of its rocket sites—often located in urban areas—and deflect attention from their own actions, while painting a picture of Israel’s disproportionate response to the kidnapping the two IDF personnel. There are two examples of how the media became a conduit of Hizballah’s deception plans: through Hizballah’s internal media, Al-Manar; and through external media such as CNN, and other world networks. Al-Manar had long been Hizballah’s primary propaganda tool; one journalist goes so far to say that “Al-Manar was to Hizballah what Pravda was to the Soviet Union.” In Hizballah’s preparations for another conflict with Israel, expanding Al-Manar’s coverage

area became a key part of their defense; it could now reach out via satellite broadcasts to Israel and much of the Arab world.

Satellite broadcast of Al-Manar began on 25 May 2000, coinciding with the day that Israel pulled its last forces out of southern Lebanon, and as Avi Jorisch describes, “came to signify freedom from Israeli occupation.” By the summer of 2006 Israelis could turn on their televisions and be exposed to daily propaganda broadcasts from Beirut including *My Blood and the Rifle*—highlighting Hizballah fighters who died fighting against Israel—and *The Spider’s House*, a talk show pointing out both “the weakness of the Zionist entity.” Al-Manar’s reporting skills had also developed over the years. Long before the US picked up the concept of embedded reporters, Hizballah placed Al-Manar reporters inside elements of the group’s Islamic Resistance militia. Schliefer highlights this as a key channel of communication for Hizballah’s PSYOP capability, and goes so far as to sum up Hizballah’s propaganda machine thusly: “If you haven’t captured it on film you haven’t fought.” Furthermore, he adds that “Hizballah... regarded the video... as an object of operation” and

that in the run up to the 2000 Israeli withdrawal saw how it was possible to net large military and psychological dividends from a video camera and a patrol. By summer 2006, Al-Manar had mastered this technique, placing its reporters—who many believed were trained fighters—into guerrilla units, having them record the battles and then broadcasting the material around the region. Even more interesting is the fact that other networks such as Al-Jazeera and Al-Arabiya used this footage, without checking the validity of Al-Manar’s version of events. Such usage aided in Hizballah’s deception of unit locations and Katyusha rocket launching sites. In addition, pictures from the war zone often made their way to the front page of newspapers and Internet sites from sources inside the conflict area, without verification of their authenticity. Because Hizballah tightly controlled the operating environment through a variety of OPSEC activities, only the information they wanted released usually made it out of Lebanon and into news broadcasts, websites, or newspapers. Hizballah even began giving guided tours of bombed out neighborhoods, stating reporters “could only take pictures of sites approved by their Hizballah minders. Violations they were told, would be treated harshly... offending reporters would never again be allowed access to Hizballah officials or Hizballah-controlled areas.” Some reporters recognized it for exactly what it was: attempts to create and control stories. Yet few journalists did



Hizballah bunker uncovered near UN outpost.
(Israeli Defense Forces)

anything about this, and continued to tell Hizballah's narrative to the world, whether it was true or not. This theme resonated disproportionately, seen across the world from Yahoo News to CNN and from Al-Jazeera to the BBC. Content analysis from Harvard's Shorenstein Center on the Press, Politics and Public Policy found in repeated surveys that based on media content in various outlets both in the Middle East and in the West, Israel was consistently labeled the aggressor in the conflict. Hizballah did this to deceive the masses about what was really happening: the kidnapping of two Israeli soldiers, the daily rocket attacks against Israeli from inside populated areas, and Hizballah's own tactics for fighting the war. Unlike other deception operations Hizballah utilized, this one would have mixed results.

The information age truly puts an emphasis on the individual and even the populace as the centers of gravity or target audiences in conflicts. No longer are they purely military-on-military battles, but the possibility exists that every single person with access to a cell phone or computer can contribute to the war effort—as witnessed in the summer conflict. With one audience Hizballah's media deception proved very effective; with another it was exposed for what it was: a fraud. Following the initiation of hostilities Hizballah was publicly rebuffed by many Arab states (to include Saudi Arabia, Jordan and Egypt) for kidnapping two IDF soldiers, describing the action as “reckless” and full of “adventurism.” However, these countries' populaces did not share the same opinion. As the conflict wore on and Hizballah continued to stand up to Israeli air and ground attacks, many of the same governments found themselves in trouble. A growing schism developed between the governments who had earlier rebuffed Hizballah, and their people. In the midst of the conflict Faiza Ambah of the *Washington Post* stated that in respect to the conflict that for these Arab governments that “each day the assault continues, they lose popularity and the respect of their people.” Hassan Nasrallah became a hero across countries

like Egypt and Jordan as people took to the streets in support of Hizballah, and to denounce their own governments for not supporting the extremist group. As hostilities continued, public opinion forced these same governments to reverse course on earlier statements and try to take an uneasy middle ground, while distancing themselves from both Israel and the United States. Jordan dispatched medical teams to Lebanon to help the “victims of Israeli aggression” while Saudi Arabia threatened to pull the plug on a 2002 peace plan between Arab states and Israel.

While the Arab states fell for Hizballah's ploy, something very different happened in the United States. If there are three names to remember for the summer conflict, they will probably be Hizballah Leader Hassan Nasrallah, Israeli Prime Minister Ehud



Figure 1. A “doctored” Adnan Hajj photo. (Reuters)

Olmert, and photographer Adnan Hajj. While Nasrallah and Olmert will be remembered for their roles as leaders, Hajj will probably be remembered for something very different.

Working for Reuters, Adnan Hajj took the photographs in Figure 1: the first being the original and the second being ‘doctored’ and sent out across the wire services. Shortly after the photo was published, the website *Little Green Footballs* ran an entry questioning the authenticity of the photo. This website, already popular for exposing the fraudulent memos regarding President Bush's career in the Air National Guard, which ultimately forced Dan Rather to resign from CBS News, again struck a coup of sorts. Within days Reuters pulled these photos, and all photos Hajj had

taken, and issued an apology. While it is unclear whether or not Hajj was working for Hizballah, the fact remains that he was attempting to execute his own deception operation which supported Hizballah's overall objectives. This was not the only time this occurred during the conflict; several bloggers banded together against other reportedly doctored photographs taken in Lebanon to combat what they saw as the “lamestream media.” This incident showed a powerful new tool in combating deception in the information age. If journalists were part of new weapons systems, then bloggers are now finding themselves in a role “as a club against the entire mainstream media.” In an interview, Ravi Nessman of the Jerusalem office of the Associated Press asserts that the influence of bloggers “was unprecedented” in this conflict and that when the bloggers [in the US] discovered that photographs had been doctored, “the credibility of the bloggers... skyrocketed and our credibility plummeted.” Hizballah's use of deception finally met a speedbump.

The use of information technology is not a traditional deception operation. But in evaluating this deception tactic, it is possible to see how the information age is producing new opportunities for deception in warfare. First of all, Hizballah took measures to simultaneously condition different targets' beliefs, quite apparent in the responses of US versus middle eastern audiences to the media narrative. Specifically, Hizballah's story influenced those governments once seen as hostile to the organization at the onset of hostilities, to reverse their opinions.

This leads to the final objective set forth by Daniel and Herbig: being able to benefit from the deception. Hizballah profited from the targets' actions not only through direct aid—as was the case with Jordan—but in further isolating Israel through Saudi Arabia's actions. While in the West, the rise of bloggers had a reverse effect on the populace, and in fact helped challenge the media's role in the deception outright—something never been seen before in a conflict. Deception type in this case would fall into the category of ambiguity, increasingly

because of the varied audiences and global network of ideas readily available to the masses—no one was really sure what to believe.

Examining the types of deception, this example lies in the realm of false and planted information. Hizballah controlled the story and what was published, and could often be found working behind the scenes to ensure the story was perfect. In essence, they created their own television show to be broadcast around the world via more mainstream media channels. On the final aspect of sensors in this deception, it is becoming ever more apparent in the information age a new sensor now exists—unaddressed before in military operations:

the individual. How an individual responds to the story and the networks, and comes together with others to make their voice(s) heard, is clearly a new type of sensor. This challenges the existing information flow structure, particularly intelligence service bureaucracies, as a key means of influencing decision makers. Altogether this is a mixed case of deception, because what worked to change the minds of leaders in the Middle East failed dramatically in the United States. The use of the media as a tool for deception, and its challenge from networked individuals, clearly shows a new instrument of war in the information age. Table 4 summarizes this deception operation.

Hijacking The Internet

The final case of deception focuses on deceit in cyber conflicts. Like the media, cyberspace is a newer nontraditional area for deception, and like the media it was the work of individuals outside of state run institutions who stood up to challenge these deceptive acts. As Israel mounted its bombing campaign against Hizballah in the summer of 2006, one of the prime targets became not only the headquarters of Al-Manar television, but

many other supporting facilities such as antenna and broadcasting sites. Despite repeated attempts by the IDF to put the television network out of commission, Al-Manar broadcast continuously from hidden locations—and even thwarted hacking attempts by IDF intelligence corps elements. Ultimately, the IDF's hacking campaign only affected the internal Lebanese broadcasts of Al-Manar, but the rest of the Arab street maintained an uninterrupted satellite feed for the duration of the war.

This cyber war between IDF hackers and Al-Manar pushed the conflict into a new arena. Hizballah turned to hiding and hijacking on the Internet in an attempt to

found at that IP address, and the hijack is complete. If the hijack goes undetected, the IP address can be linked to a new domain name, opening up the site to anyone who might search online for Al-Manar content.

In the past, many companies would not realize such a takeover occurred, and groups such as Hizballah could get away with it. This tactic proved very useful for terrorists or insurgent groups to continue to get their messages out, even if it was impossible to do so from their home countries. While similar instances of cyber deception worked in the past, this time it failed due to the work of networked groups like the Society

Criteria	Evaluation
Three Objectives? - Condition the target's beliefs? - Influence the target's actions? - Target's actions must benefit the deceiver?	- Through al-Manar & other new agencies on the ground, Hizballah painted its story to the world. - Arab audiences were convinced of Hizballah's actions and it reversed the attitudes of the governments.
Sensors targeted?	The media, also the individual.
Type: M-type or A-type?	M-type: Hizballah sought to mislead audiences and decisionmakers from their true actions inside Lebanon.
9 Characteristics? (concealment, camouflage, false and planted information, ruses, displays, demonstrations, feints, lies, and insight)	False and planted information: Hizballah only showed the reporters what they wanted, the reporters broadcast the facts that they had.

Table 4. Evaluation of the Media

restore its message of resistance. Hilary Hylton of *Time* researched this aspect of Hizballah's information plan, and found that militant Lebanese hackers searched the Internet for vulnerable sites to hijack, and then communicate with one another. She states "Hizballah uses these Web sites to run recruitment videos and post bank account numbers where supporters can donate funds" and that these communications portals are "critical as Hizballah tries to get its global message out to the world." One hijacking occurred on a US South Texas cable company: Al-Manar linked to the small cable company's internet protocol (IP) address—essentially adding an extension to their telephone line, allowing message traffic to flow. Hizballah then gets the word out through e-mail and blogs that they can now be

for Internet Research, "an informal consortium of self-described 'freelance counterterrorists' who sit in home offices and dens tracking jihadist activity on the Internet." It was this group that tracked Hizballah's web activities to the Texas cable company and notified US authorities, who in turn shut down the IP address. As a result, Hizballah's Al-Manar was forced to look for other IP's until its own could be re-established after the

war. While this case of cyber-hijacking is not as strong a deception case as the previous examples, it still deserves mention—it shows the lengths groups like Hizballah will go to in an effort to put out their messages. Examining deception type criteria, this action does not meet the idea of conditioning a target's beliefs; rather it is simply an act designed for the deceiver to hide within the target, and maintain some level of cover and concealment. Furthermore, there is no influence aspect to the target's actions. However, by having an open IP address the deceiver is able to benefit from the target's actions. This case is best considered in the category of concealment or camouflage, yet does not fit into either of the two types of deception identified: neither ambiguity increasing, nor misleading. Therefore,

Criteria	Evaluation
Three Objectives? - Condition the target's beliefs? - Influence the target's actions? - Target's actions must benefit the deceiver?	- IP addresses in cyberspace for its al-Manar websites. - Networked groups around the US looked for and found these hijacked sites.
Sensors targeted?	The only sensors targeted were unknowing ISPs who had no idea what Hizballah was doing.
Type: M-type or A-type?	Neither type fits into this criteria for deception because it success lies in staying hidden.
9 Characteristics? (concealment, camouflage, false and planted information, ruses, displays, demonstrations, feints, lies, and insight)	Concealment: Hizballah hid from plain view and known IP addresses after Israel destroyed many of their support facilities in Lebanon.

Table 5. Evaluation of Internet Hijacking


this case provides the possibility for a new type of deception—one in which the deceiver attempts pure concealment.

Regarding sensors, cyber hijacking primarily rests on the host leaving its systems' back doors open for these hacking bodies to exploit. Finally, the case of cyber hijacking reinforces the power of the individual or networks to counter this and similar threats in cyberspace. While seemingly a weak form of deception within the cyber warfare realm, the fact that networks like the Society for Internet Research are patrolling the Internet on their own—without government involvement—shows another prime example of how the information age empowers traditional noncombatants. The cyber fighters take matters into their own hands, and counter deception from the comfort of their own homes. Table 5 summarizes the Internet hijacking case, demonstrating how concept of deception still plays out in cyberspace today.

Conclusion

The preceding paragraphs present several cases of deception from the Israel-Hizballah conflict, along with supporting information on how Hizballah managed to deny Israel many of their traditional sources of information. This allowed Hizballah to dominate Israel, in ways unforeseen only a short time ago. Traditional forms of deception are still very applicable to modern warfare, while at least one of the last two cases shows

how using the media is transforming deception in the information age. The last instance of Internet hijacking shows how groups like Hizballah hide in cyberspace, utilizing unknowing targets to further their objectives.

There are still key lessons to be learned and applied regarding deception in these types of conflict. Regardless of how Israel may portray its accomplishments during the recent conflict, including destruction of Hizballah's missile capabilities and reducing the organization's ability to wage war, Hizballah still managed to spin a story of success: an IO campaign ripe with deception. Delivery of the deception signal to sensors, and that signal's interpretation by not just traditional agencies but by networked individuals, has become as important as bullets fired at the enemy. Hizballah realized the importance of the concept, and employed it fervently in this conflict. Forces around the world must be aware of these deception tactics and methods less they face the same fate as Israel; the clock is ticking. 

*Bibliography/references for this article are on the IO Sphere Home Page at:
[https://www.jiowc.osis.gov/
 Publications/IOSphere/index.cfm](https://www.jiowc.osis.gov/Publications/IOSphere/index.cfm)
 Click on the "updates" link under the
 Winter 2008 issue*